MODELS OF FORMAL GROUP LAWS OF EVERY HEIGHT

CATHERINE RAY

1. Acknowlegements

Thanks to Kazuya Kato for building these varieties, and Sean Howe for helping me understand them (which took me ages, his patience and persistence kept me going). Thanks to Aaron Slipper and Achim Krause for walking me through some of the basic number theory involved in the splitting of the p-divisible group via the splitting of the prime. Thanks to the 2017 Talbot Workshop for encouraging me to finally finish up this paper which has been sitting around for a year, and Andy Senger for pointing out that I was adding instead of multiplying. Thanks to Ken Ribet for outlining the base change from $\mathbb{C}$ to $\overline{\mathbb{F}_p}$. Finally, thanks to Peter May for listening to me rant about formal group laws for months.

Contents

2. In this work

These notes began as my way of attempting to understand examples of abelian varieties (over finite fields) whose formal group laws posess higher height. Indeed, the notion that *the height of a formal group law encodes the symmetry of the underlying abelian variety* is a notion that I found irresistibly attractive to attempt to make precise and explore with examples.

I wish to mention that this set of examples is different than those of Gorbunov-Mahowald, as they define varieties with formal group laws of height $p-1$ for every prime p.

To create formal group laws of higher heights $h \geq 3$, we will need to look at varieties of dimension higher than one by Cartier duality [1].

To find formal group laws of dimension 1, we will split these formal group laws into a formal summand, and prove that there exists a height h component of dimension 1.

This paper will construct examples of abelian varieties whose formal group laws are of higher height, prove they are Lubin-Tate. This is motivated by a computation in algebraic topology, but is of independent interest.

Remark. I wish to argue for a indirect construction of the variety which gives us formal group laws of higher height. We use the philosophy that if one is unable to directly construct local things, one can instead construct a global thing and completing/specializing to get the desired local thing.

There are *many* global things that specialize to the same local thing. We choose the variety $\mathbb{C}^m/\mathbb{Z}[\zeta_N]$ as our global model because its endomorphism ring is very simple[2] – it is (and at the very least contains) $\mathbb{Z}[\zeta_N]$, and its automorphism group is $\mathbb{Z}[\zeta_N]^\times$. For N prime, by Dirichlet's unit theorem, $\mathbb{Z}[\zeta_N]^\times \simeq \mathbb{Z}/NZ^\times \times \mathbb{Z}^{(N-3)/2}$

3. How to use the splitting of a prime to decompose your variety

The catchphrase to keep in mind is: construct formal group laws of higher height by constructing abelian varieties with larger endomorphism rings, then splitting appart those abelian varieties via the splitting of a prime.

[1] We represent p-divisible groups as a finite product of $G_{r/s}$ where r is their dimension and s is their height, and the Cartier dual of a p-divisible group takes $G_{r/s} \mapsto G_{s-r/s}$. If we request a p-divisible group with a piece of dimension 1 height 3, we wish for $G_{1/3}$ but since abelian varieties admit polarizations, the p-divisible group must be its own Cartier dual, it must be of the form:

$$G_{1/3} \times G_{2/3}$$

so it's total dimension is 1 + 2 = 3. Thanks to Andrew Salch for this explanation.

[2] Unless it is what Taniyama-Shimura call degenerate, then the endomorphism ring is a little more complicated.

3.1. **Defining the variety in characteristic 0.** First, we define our variety in characteristic 0. This is a basic construction of Taniyama-Shimura to get abelian varieties of complex multiplication type. Let A be a complex manifold $\mathbb{C}^g/O_K$, of dimension g, with an action of O_K, where $[K:\mathbb{Q}] = 2g$. Let K be a CM-field.

Remark. Here K must be a CM-field in order to have the manifold $\mathbb{C}^g/O_K$ admit a Riemann form.

Let K_0 be a totally real number field of degree g, in our case, we take $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, let K be a totally imaginary extension of K_0 (in our case, $\mathbb{Q}(\zeta_7)$), and let O_K be the ring of integers of K.

Since K is totally imaginary, the embeddings into $\mathbb{C}$ come in conjugate pairs. We pick g non-conjugate embeddings of K into $\mathbb{C}$: $\sigma_1, \cdots, \sigma_g$.

We embed $O_K \hookrightarrow \mathbb{C}^g$ by $a \mapsto (\sigma_1(a), \cdots, \sigma_g(a))$.

Lemma 1. *A is an abelian variety.*

Proof. By Silverman, a complex manifold $\mathbb{C}^g/\Lambda$ is an abelian variety over $\mathbb{C}$ iff it admits a Riemann form. Our variety indeed admits a Riemann form. Let ξ be an element $\mathcal{O}_K$ such that $-\xi^2$ is a totally positive element of K_0 (where $K_0 = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, we choose $\xi = \zeta_n - \zeta_n^{-1}$).

By [2] pg. 93, there is nondegenerate form on the torus C^g/Λ defined by: $B(z,w) = 2\sum_{j=1}^{g} Im(\sigma_j(\xi))z_j\overline{\omega_j}$ □

The CM-type of this variety is the description of the action of the endomorphism group of the variety on the tangent space of the variety which I'll call Lie A, it gives a spectral decomposition of the action of the number field K. In this case, the CM-type is simply $\sigma_1, ..., \sigma_g$.

3.2. **Base change outline.** You may righteously ask – why are we starting over char 0 in order to define thing of higher height? Height only makes sense over char p, what nonsense! We will in the end use a theorem about abelian varieties with a CM action by a finite extension of $\mathbb{Q}_p$, over a characteristic p field.

The process of base change from this initial $A(\mathbb{C})$ we will outline, as it confused the author to no end.

We begin with a variety $A(\mathbb{C})$ with an action of $\mathbb{Q}(\zeta_n)$ and show that we may present it as $A(\overline{\mathbb{Q}_p})$ with an action of $\mathbb{Q}_p(\zeta_n)$. Then, if the variety has good reduction, we may extend to a variety $A(\overline{\mathbb{Z}_p})$ (and by the functoriality of the Neron model, this still carries the action of $\mathbb{Q}_5(\zeta_n)$). Then, we may look at a special fiber of $A(\overline{Z_p})$ to get $A(\overline{F_p})$, the characterstic p model we were looking for all along [5].

3.3. **Idempotent decomposition based on splitting of the prime.** Now that we've defined the variety in characteristic 0, we will split apart the variety on the level of its p-divisible group by tensoring with a prime and looking at how the action of Fröbenius splits.

Our abelian variety A is defined over some K' (a finite extension of $\mathbb{Q}$ [3]) with an action of O_K. We look at the p^n torsion points of $A(K')$:

$$A[p^n] \subset A(\overline{\mathbb{Q}})$$

Remark. $A[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{2g}$

There is an action of O_K/p^nO_K on $A[p^n]$, indeed, $A[p^n]$ is a free O_K/p^nO_K module of rank 1.

We will use the splitting of the prime p in O_K in order represent our p-divisible group as a sum (i.e., break up our p-divisible group into smaller dimensional pieces):

Given $p \in \mathbb{Z}$,

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

in O_K. We think of the number 1 as being $1 = \sum_{i=1}^r e_i$, where

$$e_i = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

where 1 is in the ith position.

Further,

$$\begin{aligned} O_K/p^n &= \prod_{i=1}^r O_K/(\mathfrak{p}_i)^n \\ &= \bigoplus_{i=1}^r e_i O_K/p^n \end{aligned}$$

In this way:

$$A[p^n] = \bigoplus_{i=1}^r e_i A[p^n]$$

where $e_iA[p^n] = \ker(\sum_{j \neq i} e_j : A[p^n] \to A[p^n])$.

That is, we decompose $A[p^n]$ into idempotents, and this decomposition comes from the splitting of the prime p in O_K.

Note also that each part of the p-divisible group is an O_K-module, and the action of O_K preserves this splitting.

[3] the reflex field, though I think this notion is distracting from the point.

4. How to deduce the dimension and height of the formal group law

We earlier decomposed our p-divisible group into

$$A[p^n] = \bigoplus_{i=1}^{r} e_i A[p^n]$$

.

To deduce the dimension of the formal group law associated to $e_i A[p^\infty]$ over $\mathbb{F}_p$, we use the CM-type, and the Taniyama-Shimura formula. Here, we are treating our variety as living over $\overline{F_p}$ and having complex multiplication by a finite extension of $\mathbb{Q}_p$. Then:

$$\frac{\#(\text{orbit}_{\mathfrak{p}_i} \cap \text{CM-type})}{\#(\text{orbit}_{\mathfrak{p}_i})} = \frac{\text{dimension}(F_i)}{\text{height}(F_i)}$$

Here, $\text{orbit}_{\mathfrak{p}_i}$ is defined as the elements in the subgroup $Gal(K_{\mathfrak{p}_i}/\mathbb{Q}_p)$ of $Gal(O_K/\mathbb{Q}_p)$. We use F_i to denote the formal group law associated to the p-divisible group $e_i A[p^\infty]$ (that is, F_i is the connective component of $e_i A[p^\infty]$).

Note that it makes makes good sense to look at CM-type while talking about $A[p^n]$, the tangent space of of $A(\mathbb{Q}_p)$ agrees with the tangent space of the p-divisible group.

Remark. The resultant formal group law lives over the reflex field K' of the CM-pair.

5. Example: Height 3 Case

Given a height 3, we wish to construct an abelian variety whose formal group law splits into a one-dimensional component and an $(n-1)$-dimensional component, and this one-dimensional component is height 3. We do this as follows:

Let $K = \mathbb{Q}(\zeta_7)$. Let A be the three dimensional abelian variety $\mathbb{C}^3/\mathbb{Z}[\zeta_7]$ over $\mathbb{C}$ where $\mathbb{Z}[\zeta_7]$ is embedded in $\mathbb{C}^3$ by the following three homomorphisms:

$$\begin{aligned} \Phi : K &\to \mathbb{C} \times \mathbb{C} \times \mathbb{C} \\ a &\mapsto (\sigma_1(a), \sigma_4(a), \sigma_5(a)) \end{aligned}$$

Here, σ_a is the homomorphism $K \to \mathbb{C}$ which sends $\zeta_7 \mapsto {\zeta_7}^{\text{a}}$.

To be gruesomely explicit, we are thinking of the lattice $\Phi(\mathbb{Z}[\zeta_7]) = \mathbb{Z}\{\Phi(1), \Phi(\zeta_7), \Phi(\zeta_7^2), \Phi(\zeta_7^3), \Phi(\zeta_7^4), \Phi(\zeta_7^5)\}$.

Remark. We can here, for $\sigma_{i_1}, \sigma_{i_2}, \sigma_{i_3}$, choose any non-conjugate collection.

Then A has an action ("has complex multiplication") by $O_K = \mathbb{Z}[\zeta_7]$. Let p be a prime number such that $p \mod 7 = 2$ or $4 \mod 7$.

We choose this p becase $\langle p\rangle \subseteq (\mathbb{Z}/7\mathbb{Z})^\times$ is a subgroup of order 3 (i.e., $2^3 = 4^3 = 1 \mod 7$). Thus $\mathbb{Q}(\zeta_7) \otimes \mathbb{Q}_p \simeq K \times K$ where K is the unramified extension of $\mathbb{Q}_p$ of degree 3. We call the first K_1 and the second K_2.

Remark. This splitting into degree 3 components in the case $p = 2$ is due to the splitting of $\phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ when we tensor with $\mathbb{Q}_2$. We can see that $\phi_7(x) \equiv (x^3 + x^2 + 1)(x^3 + x + 1) \mod 2$, we check the derivative condition, and we apply the Hensel lemma to lift this splitting to $\mathbb{Z}/2^n\mathbb{Z}$ for every n.

We wish to look at the orbit of the characters in K_i, that is, we look at the action of $Gal(K_1/\mathbb{Q}_p) \subset Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ on ζ_7.

One of these orbits is the collection of all squares mod 7, that is: $(1, 2, 4)$. The other orbit is the remaining elements of $(\mathbb{Z}/7)^\times$, that is, $(3, 5, 6)$.

Recall that our CM-type is $(1, 4, 5)$:

- $(1, 2, 4) \cap (1, 4, 5) = (1, 4)$
- $(3, 5, 6) \cap (1, 4, 5) = (5)$

Thus, by $(*)$:

- $\frac{\text{dimension}(F_1)}{\text{height}(F_1)} = \frac{\#(\text{orbit}_{\mathfrak{p}_1} \cap \text{CM-type})}{\#(\text{orbit}_{\mathfrak{p}_1})} = \frac{2}{3}$
- $\frac{\text{dimension}(F_2)}{\text{height}(F_2)} = \frac{\#(\text{orbit}_{\mathfrak{p}_2} \cap \text{CM-type})}{\#(\text{orbit}_{\mathfrak{p}_2})} = \frac{1}{3}$

So, F_2 is a 1-dimensional formal group law of height 3.

Remark. Note that we could also choose the CM-type to be $(1, 3, 5)$ in which case the squares give us the $1/3$ piece.

Example 2. In the height 5 case, we can take the CM-type $(1, 2, 4, 5, 8)$ and orbits again the squares $(1, 3, 4, 5, 9)$ and nonsquares $(2, 6, 7, 8, 10)$, we also get a dimension 1 formal group law of height 5.

6. Varieties that model formal group laws of every height

Given a height h, we wish to construct an abelian variety whose formal group law splits off one-dimensional component, and this one-dimensional component is height h. We do this for a general height h.

To construct such a variety, we attempt to generalize the case of elliptic curves by quotienting copies of $\mathbb{C}$ by a ring of integers, in this case the ring of integers of $\mathbb{Q}(\zeta_N)$. The degree of the extension of $\mathbb{Q}(\zeta_N)$ over $\mathbb{Q}$ is $\phi(N)$, this is the same as the number of embeddings of $\mathbb{Q}(\zeta_N) \hookrightarrow \mathbb{C}$.

We take

$$A := C^{\phi(N)/2}/\mathbb{Z}(\zeta_N)$$

The actual embedding of $\mathbb{Z}(\zeta_N) \hookrightarrow \mathbb{C}^{\phi(N)/2}$ that we choose will depend on the height and N. We will call this embedding the CM-type of our variety A.

6.1. **Which $\mathbb{Q}(\zeta_N)$ to choose.** First, we simply show, given a height h, which N to choose.

(1) Given h even, pick a prime number N_1 such that $N_1 \equiv 1 \mod h$. Then, choose $N = 4N_1$.

(2) Given h odd, pick a prime number N such that $N \equiv 3 \mod 4$, and $N \equiv 1 \mod h$.

Remark. Note that if N is a prime number, $N \nmid h \iff N \equiv 1 \mod h$.

Remark. In the even case, we look at $N = 4N_1$ and not at N_1 because we wish to use the order 2 subgroup of $Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N)^\times$ to isolate a 1-d component, i.e., we want to make sure we can find a CM-type with intersection 1.

Let's talk about this in more detail. Let us examine how the characters of ζ_N factor through K_1. We represent each character as its splitting into (ζ_{N_1}, ζ_4). The characters that factor through K_1 which contain (ζ_{N_1}, ζ_4) are of the form $(\zeta_N^{p_k}, \zeta_4)$, for $k = 0, ..., h-1$.

By $(*)$, the number of elements in the intersection of the CM-type and the elements of ζ_N that factor through K_i is the dimension of the corresponding formal group law, i.e., $\frac{\#(\text{orbit}_{\mathfrak{p}_1} \cap \text{CM-type})}{\#(\text{orbit}_{\mathfrak{p}_1})} = \frac{\text{dimension}}{\text{height}}$. So, in order to have the CM-type have only one element in common with the orbit of K_1, we want the CM-type to contain

$$\{(\zeta_N, \zeta_4), (\zeta_N^{p^k}, \zeta_4^{-1}) \text{ for all } k = 1, 2, ..., n-1\}$$

This puts a restriction on p in the next section, this requires p to be 1 mod 4.

Remark. In the odd case, we choose N to be $3 \mod 4$ because if N is 3 mod 4, then $(\zeta_N^a)^{-1} \neq -\zeta_N^a$. Futher, if $N \equiv 3 \mod 4$, only one of a and its conjugate $N - a$ will be a square $\mod N$.

We may view the choice of N and of CM-type as the partioning of $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Our first partition is into a and the conjugates, $N - a$. Our CM-type we wish to be a transverse partition – for example a is a square mod N, a is not a square $\mod N$.

If we wish for the CM-type to intersect one of the orbits in only one spot due to theorem (*) which tells us that $\frac{\text{dimension}(F_i)}{\text{height}(F_i)} = \frac{\#(\text{orbit}_{K_i} \cap \text{CM-type})}{\#(\text{orbit}_{K_i})}$. Let's say $\text{orbit}_{K_i} = (a_1, a_2 ..., a_n)$. Then, we may pick the CM-type to be

$(a_1, a_2^{-1}, ..., a_n^{-1})$ to get $\#(\text{orbit}_{K_i} \cap \text{CM-type}) = \text{dimension}(F_i) = 1$. This is always legal by our careful choice of N above.

6.2. **Which prime p to choose.**

Now, let's talk about, given a height h and an extension by ϕ_N, which prime p to choose. These restrictions give us that nice transverse partition we are looking for.

- h is odd, find p such that p is of order h in $(\mathbb{Z}/N\mathbb{Z})^\times$
- h is even, find p such that p is of order h in $\mathbb{Z}/N_1\mathbb{Z})^\times$ and $p \equiv 1 \mod 4$.

We want a prime p such that $\langle p \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ is a subgroup of order h (i.e., $p^h \equiv 1 \mod N$), which implies that

$$\mathbb{Q}(\zeta_N) \otimes \mathbb{Q}_p \simeq \prod_{i=1}^{r} K$$

Remark. That is, it splits into r copies of K where K is the degree h unramified extension of $\mathbb{Q}_p$: these r copies come from the splitting of p in $O_K = \mathbb{Q}(\zeta_N)$ into $p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, and we label them accordingly.

Remark. In general, $r := \phi(N)/h$.

Remark. In the even case, we have the further requirement that $p \equiv 1 \mod 4$, that is, in the situation:

$$\langle p \rangle \subset (\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/N_1\mathbb{Z})^\times$$

$$p \mapsto (1, \alpha)$$

Here are the first few examples:

height h	g $= \phi(N)/2$	N	N_1	p
3	3	7		$2, 4 \mod 7$
4	4	20	5	17
5	5	11		$3, 4, 5, 9 \mod 11$
6	6	28	7	$5 \mod 7$
7	21	43		$4, 7, 11, 16, 21, 35, 37, 41 \mod 43$
8	16	68	17	$9 \mod 17$
9	9	19		$4, 5, 6, 8, 9, 12, 16, 17 \mod 19$

Remark. This method seems to work for much lower primes in the odd height case. It is of interest to modify the method to work for lower primes in the even height case.

7. Appendix: Reflex Fields of CM-pairs

The reflex field of a CM-pair is the minimal field over which the Lie algebra of your variety may be defined.

More specifically, given an abelian variety $A(k)$ it is the smallest field F such that the the Lie algebra T, naturally a k-vector space, may be thought of as an F-vector space $T(F)$ with the property that $T(F) \otimes_F k = T(k)$.

Let's define the reflex field of the CM-pair (L, ϕ). In our case, $L = \mathbb{Q}(\zeta_N)$. The reflex field $E' \subset \overline{\mathbb{Q}}$ is the fixed field of the subgroup $\{\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}) | \sigma\phi = \phi\}$ where ϕ is the CM-type. By definition, E' belongs to the Galois closure of L in $\mathbb{Q}$ (since the group fixing the Galois closure fixes all embeddings of L). Note that this Galois closure makes intrinsic sense even though L is not given as a subfield of $\mathbb{Q}$. [3]

So, we may compute the reflex field much more easily. In our case: $E' \subset \mathbb{Q}(\zeta_N)$ is the fixed field of all $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ that satisfy $n\phi = \phi$.

Example 3. In the case $\phi = (1, 2, 4)$, this fixed field is $\mathbb{Q}(\sqrt{-7})$, because $(1, 2, 4)$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ and is its own stabilizer.

Example 4. In the case $\phi = (1, 4, 5)$ or $(1, 2, 3)$, then the only n such that $n\phi = \phi$ is $n = 1$. Therefore the fixed field is everything, that is: $\mathbb{Q}(\zeta_7)$.

References

[1] V. Drinfel'd, *Elliptic Modules.*
`http://www.math.hawaii.edu/ xander/sp12_drinfeld/Drinfeld%20--%20Elliptic%20Modules%20I.pdf.`

[2] M. Hindry, J. Silverman *Diophantine Geometry: An Introduction*

[3] Notes by I.Boreico, *Lecture 2: CM-types and Reflex Fields.*
`http://math.stanford.edu/ conrad/DarmonCM/2011Notes/Lecture2.pdf`

[4] C. Bujard, *Finite subgroups of extended Morava stabilizer groups*
`https://arxiv.org/pdf/1206.1951.pdf`

[5] J-P. Serre, J. Tate *Good Reduction of Abelian Varieties*
`http://wstein.org/papers/bib/Serre-Tate-Good_Reduction_of_Abelian_Varieties.pdf`